Stewart R. Pollock (SBN 301356)
spollock@edelson.com
EDELSON PC
123 Townsend Street,
San Francisco, California 94107
Tel: 415.212.9300
Fax: 415.373.9435

Counsel for Plaintiff and the Putative Class

Additional Counsel on Signature Page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

LATISHA SATCHELL, individually and on behalf of all others similarly situated,

Plaintiff,

v.

SONIC NOTIFY, INC. d/b/a SIGNAL360, a Delaware Corporation, YINZCAM, INC., a Pennsylvania Corporation, and GOLDEN STATE WARRIORS, LLC, a California Limited Liability Company,

Defendants.

Case No. 4:16-CV-04961-JSW

PLAINTIFF'S COMBINED RESPONSE IN OPPOSITION TO DEFENDANTS' MOTIONS TO DISMISS

Date: June 16, 2017
Time: 9:00 a.m.
Room: Courtroom 5, 2nd Floor
1301 Clay Street
Oakland, California 94612

Judge: Hon. Jeffrey S. White

SUMMARY OF ARGUMENT

Defendants' motions to dismiss Plaintiff LaTisha Satchell's two-count complaint for violation of the Electronic Communications Privacy Act (the "Wiretap Act"), 18 U.S.C. § 2510, should be denied. Section 2520 provides that "any person whose wire, oral, or electronic communication is intercepted…in violation of this chapter may in a civil action recover from the person or entity…which engaged in that violation." Defendants Signal360 and GSW first contend that Plaintiff cannot state an actionable claim that her communications were intercepted because the App, rather than any single Defendant, recorded and analyzed her communications, and no Defendant was ever able to actually listen to Plaintiff's communications. Contrary to Defendant's argument, an interception does not require subsequent listening or transmitting, but rather refers to the initial capture, as the App functioned here, by redirecting Plaintiff's communications to temporarily record and analyze them. *See Noel v. Hall*, 568 F.3d 743, 749 n.9 (9th Cir. 2009). Plaintiff clearly states that the App recorded her oral communications. (FAC ¶¶ 7, 42-43, 48-49, 63, 77.) And much more importantly, this Court agreed that Plaintiff has already sufficiently pleaded "capture" of her oral communications.

Defendants Signal360 and GSW also contend that they cannot be held liable for "designing" and "programming" the App under Section 2511(a) because these allegations are best construed as manufacturing allegations under Section 2512. Defendant YinzCam likewise contends that it could not directly violate Section 2511(a) as the App's "developer." However, allegations of "design[ing], program[ing], and "caus[ing] the installation and activation" of software that intercepts are precisely the allegations that courts use to distinguish defendants actively engaged in the interception from those who passively aid or enable it. *See In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051 (N.D. Cal. 2015). Moreover, when an entity manufactures a device knowing that its functionality pivots on its ability to intercept communications, courts have found that the entity has "engaged in" the interception. *Luis v. Zang*, 833 F.3d 619, 637 (6th Cir. 2016).

Finally, the Wiretap Act provides a right of action against any defendant who "procures another person to intercept." *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1042 (N.D. Cal. 2014). Therefore, to the extent that Plaintiff cannot plead direct interception against GSW and YinzCam

(since the Court already ruled that Plaintiff sufficiently pleaded Signal360 intercepted her oral communications), she nevertheless has a claim, in the alternative, against GSW and YinzCan for procuring Signal360 to intercept her communications. Under either theory, Plaintiff states a claim that each Defendant directly violated the Wiretap Act, and Defendants' motions should be dismissed accordingly.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

United States Circuit Court of Appeals Cases:

United States District Court Cases:

Statutory Provisions:

Other Authorities:

INTRODUCTION

Plaintiff LaTisha Satchell brought suit against Defendants Golden State Warriors ("GSW"), Sonic Notify, Inc. d/b/a/ Signal360 ("Signal360"), and YinzCam, Inc. ("YinzCam") for invading her privacy and intercepting her private oral communications within the meaning and in violation of the Electronic Communications Privacy Act (the "Wiretap Act"), 18 U.S.C. § 2510, *et seq*. Before the Court are Defendants' motions to dismiss the first amended complaint (the "FAC"), which come following this Court's ruling on the sufficiency of the original complaint. The Court granted, in part, and denied, in part, the initial motions to dismiss, finding (1) that "the allegations that [the] App used the microphone to record surrounding audio, including conversations, would be sufficient to show 'capture' of the contents of an oral communication," and (2) that "the allegations regarding the manner in which Signal360 designed its beacon technology are sufficient to show that Signal360 'intercepted,' *i.e.* it acquired the contents of, Plaintiff's communications," but (3) that Plaintiff failed to allege facts to support interception of an "oral communication" as that term is defined in the Wiretap Act. (*Id.* 12-13).

Consistent with the Court's directives, the FAC shores up the two issues that were present in the original complaint. Namely, it now provides several examples (at least four) of private conversations that were intercepted by the App (FAC ¶ 49)—a point that no Defendant challenges. The FAC also now contains ample allegations to show that each Defendant (not just Signal360) is directly liable for the subject interceptions by virtue of (as to Signal360) designing the portable audio beacon technology, (as to YinzCam) integrating it into the App, and (as to GSW) implementing and operating the App as a means of tracking Warriors fans and their buying preferences. (*Id.* ¶¶ 4-9.) And, in the unlikely event Plaintiff failed to lay out enough facts to withstand Defendants' motions to dismiss based on their direct involvement in the challenged conduct, Plaintiff puts forth an alternative claim of "procurement" liability in terms of Defendants GSW and YinzCam procuring Signal360 to intercept her oral communications.

Unable to live with the Court's ruling, Defendants not only advance the same arguments (even the same cases) that this Court previously rejected, Defendant Signal360 – without so much as attempting to meet the rigorous standard – simply asks "that the Court to reconsider [its] ruling."

(Signal360 & GSW Mot. 9.) In that regard, all of the Defendants attempt to have the Court revisit the question of what it means to "intercept" an "oral communication" and whether it requires the contents of the communication to be listened to or otherwise processed. But the Court, consistent with Circuit and district court precedent, already ruled that an interception occurs at the point of capture or redirection irrespective of what is done with the communications afterward. (Order 13.) Defendants cite no new authority and offer no new facts that would warrant the Court revisiting – let alone reconsidering – its prior ruling on this point.

Next, all three Defendants attempt to recast Plaintiff's allegations as "aiding or abetting" in order to hide behind case law barring secondary liability under the Wiretap Act. Defendants likewise attempt to recast Plaintiff's "design" allegations as claims against the App's sellers and manufacturers under § 2512, again in an effort to minimize their respective roles in the App's interceptions and deprive Plaintiff of a private right of action. However, Plaintiff is not suing the phone manufacturer, microphone developer, or any other entity that may have aided Defendants by passively enabling the App to function. Rather, Plaintiff seeks to hold all three Defendants liable on account of the fact that they jointly designed, developed, and implemented the App knowing that its functionality pivoted on its ability to intercept communications. On that basis, she states a claim against all three that gives rise to civil liability, whether the claim stems from §2511 or §2512.

Finally, if Plaintiff is unable to state a direct claim of interception against GSW and YinzCam, she nevertheless states an actionable claim, in the alternative, against them for procuring Signal360 to intercept her oral communications. That is, Defendants YinzCam and GSW cannot hide behind Signal360's Bug when the Bug couldn't have functioned without their knowing participation.

For all these reasons, Defendants' motions should be denied in their entirety.

STATEMENT OF FACTS

A. The Original Complaint.

As alleged in Plaintiff's original complaint (*see* Dkt. 1), Defendants GSW, Signal360, and YinzCam worked together to bring basketball fans a mobile application—the "App"—that lets fans follow the Golden State Warriors NBA team and, at the same time, provides GSW with a method to

follow its consumers. (FAC ¶¶ 2, 4.) The App features portable audio beacon technology[1] that detects and responds to Signal360's unique audio signals that Signal360 generates through speakers scattered throughout various locations. (*Id.* ¶ 27.) For the App to "hear" and respond to these unique audio signals, it must constantly access the microphone on the smartphone on which it runs and must record all background audio at all times. (*Id.* ¶¶ 28, 42.) Accordingly, when the App is opened, it activates the Bug, which commands the user's microphone to constantly monitor for Signal360's beacons—i.e., as a user moves from place to place, engages in conversations, etc. In order to detect the Signal360 beacons, the Bug analyzes (and temporarily records) all background audio. (*Id.* ¶ 44.) Once the App user comes within range of a Signal360 speaker, Signal360's speaker communicates a command to the App, the user's microphone detects it (i.e., among all the other audio sounds around the user), and the Bug records it, analyzes it, and commands the App to respond accordingly, for example, by displaying banner advertisements to the consumer or by chronicling the consumer's location for later analysis. (*See id.* ¶ 43.)

To assure constant surveillance, the App must continuously capture a smartphone's audio input, even if a user isn't actively using the App itself. Thus, the App continues recording and analyzing all of the microphone's audio input until the App is completely closed—that is, when the consumer shuts off his/her smartphone or "hard closes" the App (e.g., by manually stopping the Signal360 process). (*Id.* ¶ 44.) That is to say, the App, by design, "listens" to and records a microphone's audio input even when the consumer is not actively using the App, but merely has the App running in the background of his or her smartphone. (*Id.*) The App does not seek users' permission to access their microphones for this purpose. (*Id.* ¶ 41.) Nor does the App request that users "opt-in" to Signal360's beacon technology. (*Id.* ¶ 32.)

Ms. Satchell opened the App immediately after downloading it in April of 2016. (*Id.* ¶ 46.) For the next four months, until about July 11, 2016, she used the App to follow the progress of the Golden State Warriors and, thinking nothing of it, allowed it to run in the background on her

[1] As alleged in the FAC, Signal360's audio beacon technology functions just like a "bug" designed for mobile devices: Signal360's discrete block of source code turned on users' mobile devices' microphones, constantly recorded audio (including conversations), and analyzed the recorded audio per instructions developed jointly by all three Defendants (Signal360's discrete and embedded block of source code is referred to herein as the "Bug"). (FAC ¶ 7.)

smartphone. (*Id.*) Because Defendants did not explicitly seek Ms. Satchell's permission to record and analyze all detectable audio, she had no idea that her private conversations were being surreptitiously recorded and analyzed. (*Id.* ¶¶ 48, 51.) During this timeframe, Ms. Satchell carried her smartphone on her person. (*Id.* ¶ 48.) The App—running continuously in the background—used her smartphone's microphone to record and contemporaneously analyze all background audio as Ms. Satchell traveled to various locations, where she engaged in conversations (*id.* ¶ 49) which she expected to remain private (*id.* ¶ 50).

Plaintiff filed her original complaint on August 29, 2016 against Signal360, YinzCam, and GSW. (Dkt. 1.) These three Defendants were joined in the lawsuit for a simple reason: none of the Defendants, acting alone, could have independently brought consumers a product featuring portable audio beacon technology (that was Signal360), integrated into a smartphone application (that was YinzCam), and delivered to an existent and eager user base (that was GSW). (*Id.* ¶¶ 4-9.) Together, however, Defendants were able to co-opt thousands of consumers who already downloaded the App and convince thousands of additional consumers to install a constant listening device on their smartphone (without, of course, explaining that the App also functioned as a traditional "bug"), for the purpose of delivering those consumers highly targeted advertisements. (*Id.* ¶ 14.) On November 1, 2016, Defendants—in two separately filed motions—moved to dismiss the original complaint on grounds that (i) Plaintiff lacked standing to bring her interception claim, and (ii) Plaintiff failed to state a claim for violations of the Wiretap Act, wherein each Defendant contended that the App's alleged interceptions could not be traced directly to their respective conduct. (Dkts. 26, 28.)

B. The Court's Prior Order.

On February 13, 2017, the Court delivered its Memorandum, Opinion, and Order granting, in part, and denying, in part, Defendants' motions to dismiss. (Dkt 54 (the "Order"). On the standing issue, the Court found Plaintiff had no trouble establishing Article III standing for the alleged Wiretap Act violations. (Order 9.) Turning to the argument that Plaintiff failed to state an *actionable* claim for interception (i.e., one that could be traced back to Defendants under § 2520), the Court concluded that "the allegations that [the] App used the microphone to record surrounding audio, including conversations, would be sufficient to show 'capture' of the contents of an oral

communication," (*Id.* at 12), and that "the allegations regarding the manner in which Signal360 designed its beacon technology are sufficient to show that Signal360 'intercepted,' *i.e.* it acquired the contents of, Plaintiff's communications." (*Id.* 13 (citing *Amati v. City of Woodstock Illinois*, 829 F. Supp. 998, 1008 (N.D. Ill. 1993).) However, the Court found that the original complaint lacked allegations directly linking YinzCam's and GSW's conduct to the "capture" of Plaintiff's "oral communications." (*Id.* 13.) The Court, therefore, dismissed Plaintiff's "interception" claims as to YinzCam and GSW, and granted leave to amend, allowing Plaintiff the opportunity to clarify how those Defendants, like Signal360, "are alleged to have 'acquired' the contents of an oral communication." (*Id.*)

Finally, the Court granted Signal360's motion on the narrow issue that Plaintiff did not sufficiently allege an interception of "oral communications" where she only alleged she "would" take her smartphone places where she "would" have private communications – as opposed to making specific allegations regarding private conversations in which she engaged while the App was open on her phone and, by design, recording all background audio. (*Id.* 14.)

C. <u>The Amended Complaint.</u>

Consistent with the Court's Order, the FAC now details the private conversations that were compromised. Indeed, Plaintiff now alleges four *specific* instances when Plaintiff recalls engaging in what she deemed highly private conversations while the App was open on her phone and by design (unbeknownst to her) recording all background audio. (*Id* ¶ 49.) Given the additional detail, no Defendant attacks the FAC on this basis.

On the other aspect of Plaintiff's claim, the FAC provides additional details to demonstrate that *all three Defendants* played a crucial and necessary role in creating the App and, as such, should each face civil liability for directly engaging in the alleged unlawful interceptions. Far from seeking to hold any one, some, or all of the Defendants secondarily liable for the alleged Wiretap violations, the FAC contains ample facts that establish a nexus between, on the one hand, each Defendant's involvement in the operation of an App that they knew was useful for intercepting oral communications and, on the other, the use of the App to intercept Plaintiff's communications. As further illustration, a quick summary follows of how each Defendant is directly involved in – and

vital to – the "capture" of "oral communications" within the meaning of the Wiretap Act.

Signal360 designed the App's part and parcel: the Bug. Signal360 designed the Bug to function precisely as alleged above and, as the Court already determined, " 'intercept[],' i.e. . . . acquire[] the contents of, Plaintiff's communications." (Order at 13.) The Bug's value to "enterprise customers," such as GSW, pivoted on its ability to "hear" Signal360's "proprietary, patented audio signals," (FAC ¶ 27), which could then be used to ascertain a user's precise location, (*id.* ¶ 10). However, GSW was not any typical "enterprise customer" to Signal360, but rather a partner in a trial run that, as GSW's Kevin Cote explained, provided Signal360 with "a learning experience" to improve its technology. (*Id.* ¶ 35.) To capitalize on the "learning experience" of its joint venture with GSW, Signal360 monitored the Bug's analytics through a proprietary content management system which allowed both Signal360 and GSW to "track a number of different metrics" measuring the Bug's surveillance capacity. (*Id.* ¶ 45.)

YinzCam—developer of the App—integrated the Bug into the App and knowingly programmed the App to record users' communications. As alleged in the FAC, YinzCam "developed and maintained the codebase of the [App]" and "conducted testing to ensure that the Bug would cause users' microphones to turn on and begin listening, that the [App] would work seamlessly with the Bug, and that the [App] would respond appropriately when the Bug heard a Signal360 beacon." (*Id.* ¶ 67.) Stated otherwise, without YinzCam's direct involvement, the Bug could not have engaged and begun recording—i.e., capturing—background audio and private conversations. YinzCam also programmed the App's "permissions," which left out any requests to "opt-in" to the Bug's surveillance. (*Id.* ¶¶ 31, 32.)

GSW owned the App and used it to track its fans, knowing the App would record its users' audio in the process. GSW was an active and involved partner—not to mention the primary beneficiary—in the rollout of Signal360's Bug. (*Id.* ¶¶ 33-36.) Most importantly, GSW was the party that affirmatively placed a recording device into the hands of unknowing App users. (*Id.* ¶ 29.) It also specifically employed both Signal360 and YinzCam to develop the App, knowing that its key feature was its ability to track GSW fans by surreptitiously monitoring and recording background audio. (*Id.* ¶¶ 64-65.) Signal360's Alex Bell so much as admitted that the Bug was useless without a

partner like GSW when he explained "[Signal360's beacon technology] only ever works when someone in the organization says 'I'm going to be that champion, and I'm going to grab ahold of this,' like the Golden State Warriors." (*Id* ¶ 36.) GSW—the "champion" of the Bug—was the key link among the Defendants, tying Signal360's and YinzCam's technology to its fan base, and enabling the Bug to capture Plaintiff's—and others'—private conversations for analysis.

ARGUMENT

In its Order granting, in part, and denying, in part, Defendants' motions to dismiss, the Court provided two instructions: (i) provide specific factual allegations to show that the App intercepted Plaintiff's private communications and (ii) "with the exception of Signal360 . . . [provide] the exact manner in which the other Defendants are alleged to have 'acquired' the contents of an oral communication." (Order 13.) To the first instruction, and as noted above, the FAC now provides four examples (among many others) of Plaintiff's private conversations that were intercepted by the App—a point that no Defendant challenges. (FAC ¶ 49.) With this requirement squared away, the only remaining question is not *whether* an interception took place (at least four did), but *who*—in addition to Signal360—faces potential civil liability for the alleged interceptions and, thus, "engaged" in the Wiretap Act violations at issue. And here, Plaintiff provides ample allegations to show that each Defendant (not just Signal360) is liable for the subject interceptions—along with alternative allegations of "procurement" liability with respect to Defendants GSW and Yinzcam. Defendants' motions to dismiss should thus be denied.

A. Plaintiff Meets the Legal Standard to State a Claim Against Each Defendant.

To allege an actionable interception under § 2520, a plaintiff must plead (1) that an interception took place and (2) that the defendant directly engaged in the interception. *See* § 2520(a) ("[A]ny person whose wire, oral, or electronic communication is **intercepted**…in violation of this chapter may in a civil action recover **from the person or entity…which engaged in that violation** such relief as may be appropriate.") (emphasis added). Both elements are pleaded here.

First, in terms of an interception, the Court already determined that—by design—the App used smartphone microphones "to record surrounding audio, including conversations, [which is sufficient] to show the [interception] . . . of an oral communication." (Order 12.) Because the FAC

relies on the same allegations concerning the App's design, Plaintiff sufficiently states that an interception took place.

Second, in terms of identifying the parties who intercepted or "captured" Plaintiff's private communications, the FAC provides additional allegations to show that—in addition to Signal360, who the Court already determined was liable for the App's at-issue interceptions (Order at 13)—*each* Defendant intercepted her private communications by virtue of their role in the joint design, development, and implementation of the App. And while each Defendant does its best to minimize its own liability (e.g., by attempting to downplay its role to that of a passive party), the reality is that *no* interception would have occurred but for the conduct of *each* Defendant. For that reason, each should face civil liability for the Wiretap Act violations.

B. Plaintiff Again Pleads That an Actionable "Interception" Took Place.

As this Court previously explained, the term "intercept" means that one must "*actually* acquire," (Order 10 (citing *United States v. Smith*, 155 F.3d 1051, 1058 (9th Cir. 1998))), and that an "acquisition occurs 'when the contents of a wire communication are captured *or* redirected in any way.'" (Order 11 (emphasis in original) (citing *Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009) (quoting *United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992)).)[2] After examining the case law applying these rules, the Court concluded that "allegations that the App used the microphone to record surrounding audio, including conversations, would be sufficient to show 'capture' of the contents of an oral communication." (Order 12.) Plaintiff again alleges that the App used her smartphone's microphone to record surrounding audio, (FAC ¶¶ 10, 43), including at least four private conversations, (*id.* ¶ 49). Thus, she squarely alleges that an interception took place.

Nevertheless, Defendants again challenge Plaintiff's allegations that an "interception" occurred under § 2511(1)(a), relying on the same cases they cited when they initially raised the issue in the first round of motion to dismiss briefing. Yet this Court has already engaged in an

[2] Thus, a party has intercepted a communication's contents within the meaning of the statute when it records the communication. Whether or not communications are subsequently listened to or otherwise processed is after the fact and not relevant to determining whether those communications were intercepted. *See Noel*, 568 F.3d at 749 n.9 (finding that acquisition occurs "when the contents of a wire communication are captured or redirected in any way," not subsequent listening or copying).

exhaustive analysis of those cases, articulated the legal standard, and concluded that, at least as to allegations that Signal360 recorded communications, Plaintiff has already met the standard. (Order 13 ("Plaintiff has alleged facts to show Signal360 engaged in acts that would qualify as interception under the Wiretap Act.").) The FAC retains Plaintiff's allegations that the Bug was "designed to use users' microphones" (FAC ¶ 44), and "temporarily recorded audio and retained portions of the audio for further analysis" (FAC ¶ 43), while detailing how the App was programmed by YinzCam to "instantly initiate the Bug once the App was installed and opened" (FAC ¶ 41) and how GSW identified "rules and terms for their beacon scheme" which would "cause the Bugs on those devices to activate and, thus, turn users' smartphones into listening devices." (FAC ¶ 42.) In short, Plaintiff's FAC retains her original theory of how the App works, which this Court already found adequate to state a claim of "interception."

Defendants now contend that the FAC fails to show an interception against *any* Defendant because it "fails to show that [the App] '*actually* acquire[d]' any of Plaintiff's oral communications." (Signal360 & GSW Mot. 7.) In this vein, Defendants' motions are replete with conclusory assertions about the App's functionality, despite that at this stage of the proceedings, nothing need be proven and the Court accepts as true the factual allegations in the FAC. *Lazy Y Ranch LTD v. Behrens*, 546 F.3d 580, 588 (9th Cir. 2008). Put otherwise, Defendants add nothing to the legal standard previously articulated by this Court, and thus fail to explain why the FAC's already-accepted allegations of "recording" now fail to meet it. The reason is simple: while couched as a challenge to the sufficiency of Plaintiff's *allegations*, this new argument amounts to a challenge to Plaintiff's evidence on the *merits*. Defendants' buried contention is not that the FAC failed to *allege* acquisition (because it didn't), but rather that it failed to *actually show how* communications were acquired. The argument is premature as it boils down to an evidentiary issue, not a legal one.

In short, the Court properly examined whether an allegation of "recording" sufficed to show an actionable "interception," and defendants have given no reason why the Court should revisit its ruling on this issue. *In re Yahoo Mail Litig.* is instructive on this point. 7 F. Supp. 3d 1016, 1027 (N.D. Cal. 2014). In *Yahoo*, defendant Yahoo challenged plaintiff's "interception" allegations by disputing whether the emails were "in transit," as required by law. *Id.* (citing *Konop v. Hawaiian*

Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002)). Specifically, Yahoo argued that the emails it allegedly accessed had already reached its servers, and the complaint failed to show that they were still in transit and not in electronic storage when the alleged point of access occurred. *Id.* By introducing these new factual assertions (i.e., that the emails were temporarily in electronic storage when they were allegedly accessed), Yahoo introduced the issue of whether the term "intercept" applied to *en route* storage of emails. In denying Yahoo's motion, the court refused to take up that particular issue at the motion to dismiss stage, explaining that it must accept as true plaintiffs' allegations, notwithstanding Yahoo's contentions to the contrary. *Id.* at 1027-28.

Similarly—and without citing any authority in support[3]—Signal360 & GSW here urge the Court to examine whether the term intercept requires recording communications "in some form that allowed [Defendants] to listen to those conversations." (Signal360 & GSW Mot. 7.) Defendants argue that the Court should re-examine whether an interception occurred considering that "Defendants never had access to the contents of any oral communications." (*Id*. 8; *see also* YinzCam Mot. 6.) But, again, the FAC includes allegations the Court previously found sufficient in terms of pleading an actionable interception. (FAC ¶ 42 (the App could "listen[] and pick[] up on any and all audio within range of a user's microphone."); *see also id.* ¶ 43 ("the Bug temporarily recorded audio and retained portions of the audio for further analysis. Defendants programmed the Bug to analyze and monitor the picked-up audio"); ¶ 48 ("once activated, [the Bug] turned on her smartphone's microphone and thereby caused the App to constantly record all audio, including conversations").) Just as in *Yahoo*, Defendants' argument that Plaintiff must allege they "'*actually* acquired' her oral communications *in some form that allowed them to listen to those conversations*" (Signal360 & GSW Mot. 7) is not appropriate for resolution at this stage. Because Plaintiff has

---

[3] Signal360 and GSW provide *one* fleeting reference to *Carrier IQ*, to make the point that Plaintiff does not allege the recorded conversations were sent from her phone to separate servers controlled by Defendants. (*See* Signal360 & GSW Mot. 7.) But as the Court already held, "interception" does not require that a communication be captured on one device and then be transmitted elsewhere. (Order 12 (concluding that the App's *recording* of surrounding audio was sufficient to show the 'capture' of the contents of an oral communication) (*citing Noel*; 568 F.3d at 750; *Siripongs v. Calderon*, 35 F.3d 1308, 1311, 1319 (9th Cir. 1994).) As described herein, Defendants provide no basis for the Court to re-open this finding, which only concerns the App's alleged design and functionality.

sufficiently shown that the App recorded her communications, Plaintiff plausibly alleges that the App "intercepted" them.

C. Plaintiff States a Direct Claim Against Each Defendant for Its Role in the Interception.

Given that Plaintiff adequately pleaded that an interception occurred, the remaining question is who can be held liable for it. The Wiretap Act defines "the category of defendants from whom the plaintiff may recover: those who 'engaged in that violation.'" *DirecTV v. Dillon*, No. 03-8578, 2004 WL 906104, at *2 (N.D. Ill. Apr. 27, 2004). Prior to the amendment of § 2520 in 1986, the statute specifically provided for a cause of action "against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications." *See Flowers v. Tandy Corp*, 773 F.2d 585, 587 n. 2 (4th Cir. 1985). The amended statute, however, uses broader language and now defines a potential defendant as any person who "engaged" in a violation of the chapter. By abandoning references to specific acts (e.g., "intercept, disclose, use, or procure") in favor of the more general "violation," § 2520(a) identifies a broader category of potential defendants. *See DirecTV, Inc. v. Tasche*, 316 F. Supp. 2d 783, 790 (E.D. Wis. 2004); *Luis v. Zang*, 833 F.3d 619, 639 (6th Cir. 2016).

Defendants' main attack comes in the form of attempting to recast Plaintiff's allegations as being based on secondary liability. But, that's not what's going on here. Rather, the FAC's new allegations make clear that no one Defendant, acting alone, could have carried out the interceptions about which Plaintiff complains. Because each Defendant was integral—and directly involved—in the recording of Plaintiff's communications, they are each liable under § 2520.

Defendants then attempt to reframe Plaintiff's allegations (for Signal360 and GSW, as being based on "manufacturer" liability under § 2512) (and for YinzCam, as being based on "procurer" liability under § 2511) to argue Plaintiff lacks a private right of action. But, again, Plaintiff's main claim is that each Defendant is directly liable under § 2511 for its role in the subject interceptions. And, despite the creativity in the argument, it's clear that Plaintiff is not suing the phone manufacturer, microphone developer, or any other entity that can be said to have facilitated the interceptions by passively enabling the App to function. Rather, Plaintiff seeks to hold responsible the App's joint-masterminds, each of which played a key role in causing the App to monitor users'

surrounding audio. As for procurement liability, it could certainly serve as an alternative way of holding both YinzCam and GSW liable for the App's challenged conduct.

Finally, Defendants revert to their tired—and already once rejected—standing arguments, suggesting that the harm cannot be traced to them because they did not "actually acquire" Plaintiff's communications. The Court rejected the argument that no interception took place, and it should have no difficulty linking each Defendant to the interception, given the FAC's added allegations.

1. Plaintiff does not rely on a theory of aiding and abetting.

Defendants all invoke a line of precedent that, inappositely, excludes theories of secondary liability from § 2520 of the Wiretap Act. In all of these cases, the courts held that the Wiretap Act does not create a cause of action for **aiding and abetting liability.** However, not all theories of concerted action are necessarily premised on aiding and abetting, and the theory of concerted action alleged in the FAC is based on a theory of direct participation in the scheme's *design* and thus, direct liability, as to each Defendant.

Concerted action under an aiding and abetting theory attaches liability for the tortious acts of another when someone *substantially assists* the tortious actor. Restatement (Second) Torts § 876(b) & (c) (1979). In this case, however, Plaintiff's theory of concerted action hinges on allegations that each Defendant *participated in the development and design* of the tortious action, not that YinzCam and GSW substantially *assisted* Signal360 in doing so. In other words, Plaintiff does not allege that the Bug alone (and, as a corollary, the company behind it) intercepted Plaintiff's communications, nor does it seek to hold any one Defendant liable for the actions of another. Dooming Defendants' argument, the FAC instead alleges that each Defendant played an integral role in the App's interception by way of designing the portable audio beacon technology (Signal360), integrating it into the App (YinzCam), and implementing the App as a scheme to track Warriors fans (GSW). (FAC ¶¶ 4-9.) Allegations like these, which make clear that the interceptions could not have occurred without concerted action and direct participation of each Defendant, demonstrate that the *Carrier IQ* line of cases that Defendants cite are simply not applicable to this case. Indeed, to the extent these cases bear on the issues, at best, they highlight that each Defendant's role in the

interception is more analogous to that of a software developer, rather than a passive ISP or device manufacturer.

In each of the cases that Defendants use to try to defeat Plaintiff's theory of concerted action, the plaintiffs sought to hold defendants liable as **aiders and abettors**. In *Carrier IQ*, plaintiffs sued both bugging software developer Carrier IQ as well as various "Device Manufacturers" who had the bugging software installed on their products. 78 F. Supp. 3d 1051, 1061, 1088-89 (N.D. Cal. 2015). The court dismissed the claims against the Device Manufacturers who, in its view, merely "provided a means through which [Carrier IQ] subsequently intercept[ed] communications." *Id*. at 1088. The Court upheld the claim against Carrier IQ who was alleged to have "designed, authored, programmed, and caused the installation and activation of" the software at issue. *Id.* at 1061.

Similarly, in *Valentine v. Wideopen West Finance, LLC.*, plaintiffs sued internet service provider ("ISP") WOW for installing an "Appliance" on their network facilities that enabled the Appliance developer NebuAd to intercept its users' online communications (using the Appliance). 288 F.R.D. 407, 411 (N.D. Ill. 2012). The court dismissed claims against WOW, holding that the complaint's allegations that WOW "used its network facility resources and the Appliance to divert and transfer . . . communications to the Appliance" showed only that WOW "facilitated" NebuAd's interception by diverting the communications to NebuAd. *Id*.[4] Because the theory against WOW was indisputably based on secondary liability, the Court rightly dismissed the claim.[5]

---

[4] The court in *Valentine* relied heavily on an almost identical case, *Kirch v. Embarq Mgmt Co.*, 702 F.3d 1245 (10th Cir. 2012). However, both *Valentine* and *Kirch* are of little help here because unlike an ISP defendant who facilitated the interceptions while performing its ordinary service, Defendants each made a deliberate and distinct contribution to the App's design (Signal360), development (YinzCam), and operation (GSW). *See In re Google Inc*., No. 13-02430, 2013 WL 5423918, at *8 (N.D. Cal. Sept. 26, 2013) ("*Kirch* stands only for the narrow proposition that interceptions incidental to the provision of the alleged interceptor's internet service fall within the 'ordinary course of business' exception.").

[5] *Toys R Us* is no more helpful. *In Re Toys R Us, Inc. Privacy Litig.*, No. 00-2746, 2001 WL 34517252, at *6 (N.D. Cal. Oct. 9, 2001). There, plaintiffs did not allege that website operator Toys R Us intercepted communications or procured another person to intercept, but rather that it "aided and abetted [software developer] Coremetrics in their interception." *Id.* Because Plaintiff here states direct claims against Defendants for intercepting her communications—i.e., like Coremetrics and unlike Toys R Us, each Defendant here played an integral role in devising the App that intercepted Plaintiff's communications—the *Toys R Us* holding is inapposite to this case.

The common thread in these cases is that the defendants all contributed to the operation of the intercepting device by providing an environment that *enabled* the interceptions in some sense. However, none of these defendants were alleged to have directly participated in the inner-operations of the device. That is, the complaints in all these cases distinguished the defendants from the software developers that had, in the words of the *Carrier IQ* court, "designed, authored, programmed, and caused the installation and activation of" the device that carried out the interceptions. 78 F. Supp. 3d at 1061. Moreover, not all courts agree that allowing a software developer to install an intercepting device on one's network merely serves as "aiding and abetting" in the interception. *See Mortensen v. Bresnan Commc'n, L.L.C.*, No. 10-13, 2010 WL 5140454, at *2 (D. Mont. Dec. 13, 2010) (holding plaintiffs stated a claim against ISP by alleging that "but for that Appliance, NebuAd would have been unable to access [p]laintiffs' personal electronic transmissions").

Here, Plaintiff sufficiently alleges that Defendants each engaged in conduct that directly violated the Wiretap Act by virtue of their direct participation in a joint enterprise (the App) that this Court has already found to have plausibly resulted in interceptions. (*See* Order 12 ("the Court concludes that the allegations that [the] App used the microphone to record surrounding audio, including conversations, would be sufficient to show "capture" of the contents of an oral communication.").)[6] Nothing additional need be pleaded to support that aspect of her claim.

2. Plaintiff's "design" allegations are actionable under § 2520.

The Court's previous Order clearly held that Plaintiff stated an actionable interception claim based on her "design" allegations against Signal360. (Order 13 ("The Court finds the allegations regarding the manner in which Signal360 designed its beacon technology are sufficient to allege that Signal360 'intercepted'").) Unable to accept the Court's prior Order, Signal360 and GSW now

[6] This Court previously cited *Freeman v. DirecTV, Inc.*, 457 F.3d 1001, 1005 (9th Cir. 2006) for the proposition that there is no secondary liability under the Wiretap Act. (Order 13.) Plaintiff does not challenge this reading of *Freeman*, but notes that there was no dispute in *Freeman* that plaintiffs' allegations were based on a theory of secondary liability. *See Freeman*, 457 F.3d at 1005 ("[B]ecause it is uncontroverted that neither [defendant could be held directly liable for plaintiffs' claims], the question is simply whether this statutory language creates a private right of action for conspiracy or aiding and abetting.") Here, because Plaintiff alleges direct violations of the Wiretap Act against each Defendant, there is no tension with *Freeman*.

attempt to evade liability based on that finding by insisting that "design" allegations are more appropriately reviewed under § 2512, which according to them, does not provide for a private right of action. (Signal360 & GSW Mot. 9.) Similarly, YinzCam seeks to skirt liability for its participation in the App's design by arguing that it could not have "procured" the interceptions, as it merely acted as an agent of the other Defendants, like a seller of an intercepting device. (YinzCam Mot. 10-12.) But, because Plaintiff alleges that all three Defendants jointly designed and developed the App knowing that its functionality pivoted on its ability to intercept communications, she states a claim against all three that gives rise to civil liability, whether stemming from § 2511 or § 2512.

The Wiretap Act also imposes liability under § 2512 on any defendant that "manufactures, assembles possesses, or sells" a "device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications…" § 2512(1)(b). While some courts have interpreted § 2520(a) as limiting civil liability for only alleged violations of § 2511, *see, e.g., DirecTV, Inc. v. Haupert*, 327 F. Supp. 2d 990, 994 (E.D. Wis. 2004), others have imposed liability on defendants who, while accurately classified under § 2512, also play "an active role in the use of the relevant device to intercept…plaintiff's [oral] communications." *Zang*, 833 F.3d at 637. Courts have likewise held that a defendant who is "intimately and integrally involved" with facilitating an unlawful interception—for instance, by allowing recording software to be implanted on rental computers—may also face direct liability under the Wiretap Act. *See Byrd v. Aaron's, Inc.*, 14 F. Supp. 3d 667, 690 (W.D. Pa. 2014); *Jacobson v. Rose*, 592 F.2d 515, 522 (9th Cir. 1978) (imposing liability on defendant "involved in the setting up of the recording devices").

Signal360 and GSW contend, without any authority or explanation, that Plaintiff's allegations that Defendants "designed," (Signal 360, *see, e.g.*, FAC ¶¶ 7, 44, 66) "programmed," (YinzCam, *see, e.g.*, FAC ¶¶ 4, 10, 43, 67) and wrote "rules" (GSW, *see, e.g.*, FAC ¶¶ 42, 65) for the beacon technology are "simply allegations of 'manufacture[]' and 'assembl[y]' applied to the particular context of a software program" and thus fall only within the scope of § 2512. (Signal360 & GSW Mot. 10-11.) The big problem for them, however, is that such a conclusion flies in the face of a long line of precedent finding that defendants who "designed" and "programmed" devices that

intercept communications are liable for "intercepting" under § 2511(a). *See, e.g., Carrier IQ*, 78 F. Supp. 3d at 1061; *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1037 (N.D. Cal. 2014).[7]

Likewise, YinzCam's assertions that it was a "mere secondary actor"—and the cases it relies on in support—simply serve to highlight the difference between those found to have engaged in "secondary" actions like manufacturing or selling from the conduct of Defendants in this case. *See, e.g., Flowers*, 773 F.2d at 590 (holding that an electronics company which merely sold a telephone recording device to a husband to spy on his wife could not be held liable to the wife); *Oceanic Cablevision, Inc. v. M.D. Electronics*, 771 F. Supp. 1019, 1029 (D. Neb. 1991) (holding that defendants who sold descrambling devices to plaintiff television provider's customers were not liable to plaintiff under § 2511(1)(a) but that plaintiff may still assert a private right of action for the sale of the devices under § 2512); *Greek Radio Network, Inc. v. Vlasopoulos*, 731 F.Supp. 1227 (E.D.Pa. 1990) (holding that act of selling descrambling devices did not fall within the "procuring" element of § 2511).

Nevertheless, even if the Court finds that any of the Defendants fall within the class of "manufacturers" or "sellers" under § 2512, such a finding would not doom Plaintiff's claim. To be sure, many courts have found that by providing a right of action against anyone who has "engaged in" a violation that gives a plaintiff standing under the Act, Congress contemplated that some nexus may exist between manufacturing or selling a device that intercepts and the interception itself, such that a manufacturer or seller may be held liable under § 2520 regardless of whether the manufacturer or seller itself intercepts communications. *See, e.g., DirecTV, Inc. v. Tasche*, 316 F. Supp. 2d 783, 790 (E.D. Wis. 2004) ("Though Tasche may not have actually done the intercepting himself, it would be a stretch to find that he was not 'engaged in' that act. Those who sell devices that are designed to steal DirecTV's satellite transmissions to those who are intent on stealing DirecTV's satellite transmissions are, in my view, 'engaged in' intercepting such transmissions.");

[7] Signal360 and GSW's attempt to analogize to *In re Lenovo Adware Litig.*, No. 15-02624, 2016 WL 6277245, at *1 (N.D. Cal. Oct. 27, 2016), does little to bolster its defense. Plaintiffs in *Lenovo* only sought to hold Lenovo liable as a manufacturer under § 2512. *Id.* Notably, the court in *Lenovo* took no position on whether Lenovo had any involvement in "enabling and directing the operation of" software developer Superfish's device—as Defendants Signal360 and GSW suggest (Signal360 & GSW Mot. 11)—because, unlike here, plaintiffs in *Lenovo* never made these allegations.

DIRECTV, Inc. v. Kitzmiller, No. 03-3296, 2004 WL 692230, at *4 (E.D. Pa. Mar. 31, 2004). That is, when an entity manufactures a device knowing that its functionality pivots on its ability to intercept communications, courts have found that the entity has "engaged in" the interception. *Zang*, 833 F.3d at 637.

Zang is instructive here, but not for the reasons GSW and Signal360 claim. There, after finding that a device intercepted plaintiff's communications, the Sixth Circuit examined whether defendant's alleged manufacture, marketing, sale, and operation of the device caused it to be "engaged in that violation" of the Wiretap Act. *Id.* Distinguishing plaintiff's claim from other allegations under § 2512 – which turned on whether manufacturing, sale, or possession were alone sufficient to support a private cause of action – the court found that where defendant allegedly "manufactured, marketed, and sold the [device] with knowledge that it would be primarily used to illegally intercept electronic communications" and "remained actively involved in the operation of [the device]," defendant "took a much more active role in causing the Wiretap violation in this case than the defendants in other cases," and refused to dismiss plaintiff's claims. *Id.*[8]

As in *Zang*, the issue before the Court is whether each Defendant's alleged involvement in the App's interceptions caused it to be "engaged in that violation" of the Wiretap Act when Plaintiff's communications were intercepted. Like the allegations in *Zang*, the FAC pleads facts that establish a nexus between, on the one hand, each Defendant's involvement in the operation of an App that they knew was useful for intercepting and, on the other, the use of the App to intercept Plaintiff's communications. Signal360 "distributed its software to its partners…knowing that its integration and use would necessarily record consumers' conversations." (FAC. ¶ 7.) GSW

[8] Signal360 and GSW mischaracterize the holding in *Zang* to suggest that it was the defendant's *possession* of the intercepted communications that brought its conduct within the purview of § 2520, as if to say that the defendants must "actually acquire"—i.e., intercept—the communications in order to be held liable. (*See* Signal360 & GSW Mot. 12.) However, the *Zang* court specifically found that the defendant "**itself did not initiate the specific action that 'intercepted, disclosed, or intentionally used' [plaintiff's] communications in violation of the Wiretap Act.**" *Zang*, 833 F.3d at 637 (emphasis added). In other words, the defendant in *Zang* was found to have engaged in the interception even though it did not itself intercept, i.e., acquire the communications. It was sufficient that the defendant was "actively involved in the operation of [the device]." *Id.* Thus, Signal360 and GSW's emphasis on the defendant's physical possession of the intercepted communications is misleading and irrelevant.

"understood that releasing its App with the Bug installed would…cause all audio (including conversations) to be constantly monitored and recorded." (*Id.* ¶ 8.) YinzCam "programmed the [App] to instantly initiate the Bug once the App was installed and opened." (*Id.* ¶ 41.) Given this nexus, each Defendant was "engaged" in the App's interceptions.

3. Plaintiff need not show that each Defendant "actually acquired" her communications in order to show that each engaged in the interception.

Defendants' hyper focus on which entity "actually acquired" Plaintiff's communications reflects a misreading of § 2520(a). To be sure, the Wiretap Act was drafted long before today's universe of technology could be envisioned, and, as Signal360 and GSW suggest, the "particular context of a software program" (Signal360 & GSW Mot. 10) may present an interpretive difficulty. That is, where the interception here required a series of almost instantaneous communications between the Bug's code, the App's code, the device's microphone, and the surrounding audio, (FAC ¶¶ 4-7, 9-10, 27-28,40-44), pleading one party's isolated "control" over the interception or its contents is almost certainly not required to withstand a motion to dismiss. *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1028. However, as the amended § 2520 makes clear, Plaintiff need not spell out how each Defendant "actually acquired" her communications in order to state a plausible claim, but need only show, first, that an interception occurred, i.e., that at *some point,* her communications were actually acquired (to meet the statute's standing requirement) and second, that each Defendant "engaged in" the interception. § 2520(a). *See DirecTV v. Dillon*, 2004 WL 906104, at *2.

In short, the scope of conduct considered to be the "interception" in this case *required* joint and concerted action on the part of all three Defendants. Therefore, by alleging an interception by the App and detailing each Defendant's participation in the concerted development, design, and operation of the App, the FAC alleges each Defendant directly engaged in a violation of the statute.

D. Plaintiff States a Direct Claim Against YinzCam and GSW, in the Alternative, for Procuring Signal360 to Intercept Plaintiff's Communications.

If Plaintiff cannot state a direct claim of interception against Defendants YinzCam and GSW, she nevertheless states an actionable claim that each procured Signal360 to intercept her communications, which is itself a direct violation of the Wiretap Act. § 2511(1)(a) (imposing

liability on anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept…"). While Defendants argue there is no civil liability for procuring one to intercept a communication in violation of § 2511(a), *Peavy v. WFAA–TV*, 221 F.3d 158, 169 (5th Cir. 2000), that is far from settled law. To Plaintiff's knowledge, there is no binding authority to answer the question of whether a procurer of an interception may be sued by the person whose communication was intercepted, thus presenting this court with an issue of first impression.

In *Peavy*, the Fifth Circuit reasoned that because the "procures any other person to intercept…" language had been amended out of the civil provision of the ECPA, Congress must have intended to foreclose civil lawsuits against that class of defendants. *Id*. But, the 1986 amendments to the statute evidence that Congress's intent had more to do with "update[ing] and clarify[ing] [f]ederal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies," S. Rep. No. 99-541, at 1 (1986), namely insofar as it added "electronic communication" to the types of communications within the purview of the statute (in addition to wire and oral communications). *Id*. at 26. Thus, a reasonable reading of the changes to § 2520 is that, substantively, the amendment only addressed technological changes; i.e., the inclusion of electronic communications. As one court aptly put it, the Senate's report suggests that "the changes to [the portion of § 2520 at issue here] were cosmetic rather than substantive." *Lonegan v. Hasty*, 436 F. Supp. 2d 419, 428 (E.D.N.Y. 2006) (citing S. Rep. No. 95–797, at 26–27 (1986)).

Disagreeing with *Peavy*, several courts around the country have found that the amended statute "shows no intent on the part of Congress to eliminate the private right of action for procurement violations." *Id.*; *see also Ali v. Douglas Cable Commc'ns*, 929 F. Supp. 1362, 1381 (D. Kan. 1996). In fact, even the court in *Valentine*—while declining to find a private cause of action against those who aid and abet others to intercept—found that "the text of § 2520(a) actually does authorize civil actions against those who 'procure' a banned interception." 288 F.R.D. at 412.

YinzCam seems aware of this, as it attempts to shift the blame for any "procurement" liability onto GSW, suggesting that GSW alone acted as the "principal" procurer, while YinzCam was merely an agent taking directions from the other Defendants. (YinzCam Mot. 12). Essentially,

YinzCam argues that, on the one hand, it cannot be held liable as an "interceptor" because it merely developed software that activated an intercepting device, i.e., the Bug (YinzCam Mot. 8), while on the other hand, it cannot be a "procurer" because it did so as an agent of GSW (*id*. 11-12). First, there is no basis for holding GSW vicariously liable for YinzCam's actions, as YinzCam's principal-agent logic suggests. More importantly, the Wiretap Act could not possibly allow such a loophole for software developers like YinzCam. Thus, if YinzCam's conduct as the App developer does not implicate it as one engaging in the interception, then YinzCam should at least be held accountable for procuring Signal360 to perform the interceptions. *Cf. DIRECTV Inc. v. Barrett*, 311 F.Supp.2d 1143, 1146 (D. Kan. 2004) (avoiding the question of whether § 2520 retains "procurement" liability by ruling that plaintiff's direct interception theory was sufficient to support the claims). Likewise, if Plaintiff's interception theory against GSW fails, her direct procurement theory should be enough to support her claims against it.

CONCLUSION

For all of these reasons, Defendants' motions to dismiss should be denied in their entirety. In the event this Court grants either motion, however, Plaintiff respectfully requests leave to amend her pleadings.

Respectfully submitted,

LATISHA SATCHELL, individually and on behalf of all others similarly situated,

Dated: May 9, 2017

By: /s/ Rafey S. Balabanian
One of Plaintiff's Attorneys

Rafey S. Balabanian*
rbalabanian@edelson.com
Eve-Lynn J. Rapp*
erapp@edelson.com
Stewart R. Pollock (SBN 301356)
spollock@edelson.com
EDELSON PC
123 Townsend Street,
San Francisco, California 94107
Tel: 415.212.9300
Fax: 415.373.9435

Counsel for Plaintiff and the Putative Class

**Admitted pro hac vice.*